Authentication of a Computer-based System

Possible Authentication Methods Using the Computational Block as an Example

James L. Fuller
Pacific Northwest National Laboratory

Purpose of Authentication

- To assure the monitors that the “host-supplied” equipment is making credible measurements:
  - assure that the system is assembled as designed,
  - assure that the system functions as designed,
  - assure the monitors that the host-supplied equipment does not contain a “hidden-switch” that allows the host to pass out-of-spec materials.

The Hidden-Switch Issue

- The term “hidden-switch” is used to denote any method, device, or feature in the measurement system which could be used by the host to fool the monitor.
- A “hidden-switch” could enable the host to covertly and erroneously pass selected canisters.
- A “hidden-switch” could reside in either hardware, software, or a combination of both.

Methods of Authentication

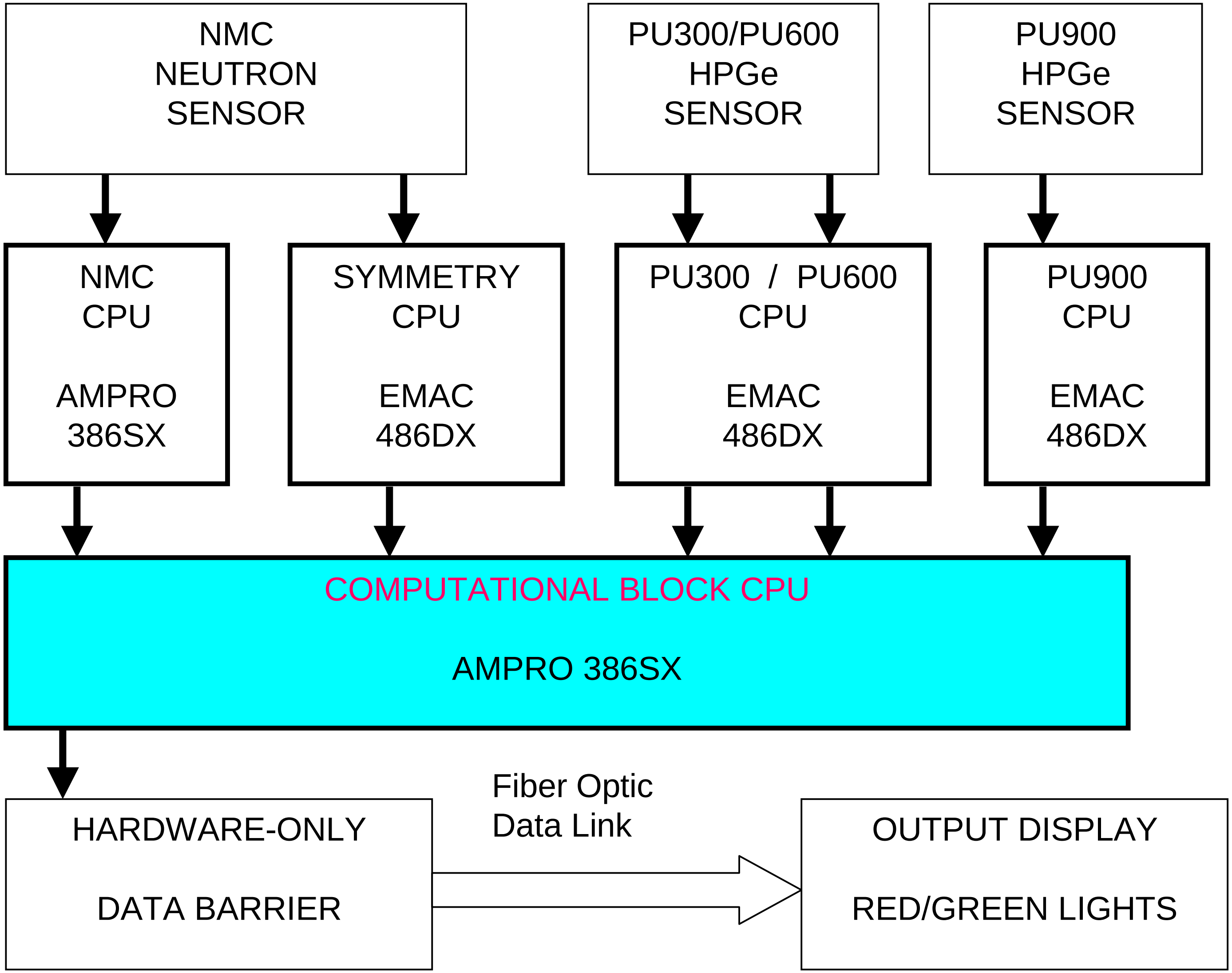
- Use of trusted, unclassified calibration sources
  – Demonstrated in the course of operating the system and subject of another presentation
- Random selection of equipment
  – Possible application for both hardware and software
- Use of Documentation
  – An especially useful confidence building tool, if random detailed examinations are allowed

Ideas on how to use random selection and documentation will be described in detail for the case of the Computational Block.

Designing for Authentication

- Select elements that support transparency:
  - availability of extensive documentation;
  - minimal or no extraneous functionality;
  - software utilizing inexpensive or publicly available source code.
- Design and engineer the system to be easily inspectable:
  - design for ease of disassembly & reassembly;
  - use printed circuits rather than wirewrap, or hand-wired circuit;
  - use two-layer printed circuits rather than multiple layers;
  - spread out elements with labels accessible;
  - use a single layer of circuit boards;
  - removable and/or transparent lids;
  - provide easy-to-use test points.
- Using identical elements reduces authentication effort.

Computational Block—Location In System



NMC
NEUTRON
SENSOR

PU300/PU600
HPGe
SENSOR

PU900
HPGe
SENSOR

NMC
CPU

AMPRO
386SX

SYMMETRY
CPU

EMAC
486DX

PU300 / PU600
CPU

EMAC
486DX

PU900
CPU

EMAC
486DX

COMPUTATIONAL BLOCK CPU

AMPRO 386SX

HARDWARE-ONLY

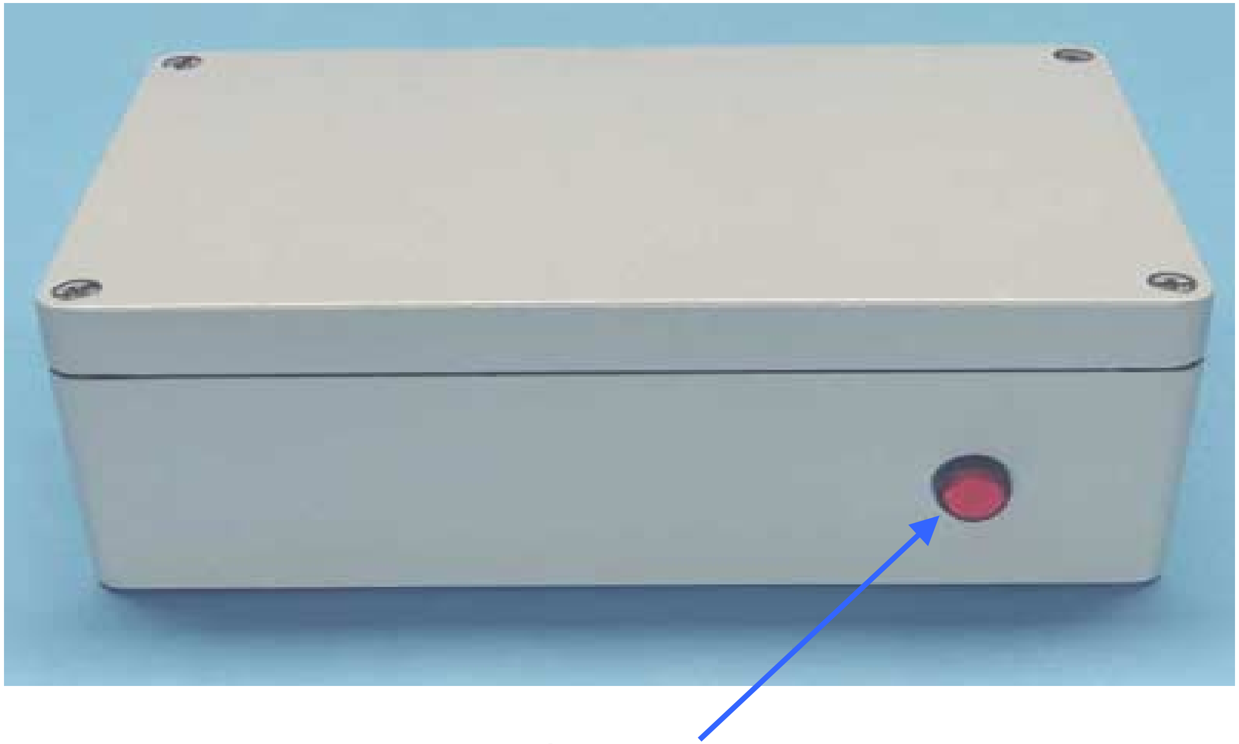
DATA BARRIER

Fiber Optic
Data Link

OUTPUT DISPLAY

RED/GREEN LIGHTS

Attribute Measurement System Computational Block



Push-Button
On/Off Switch

Computational Block Elements

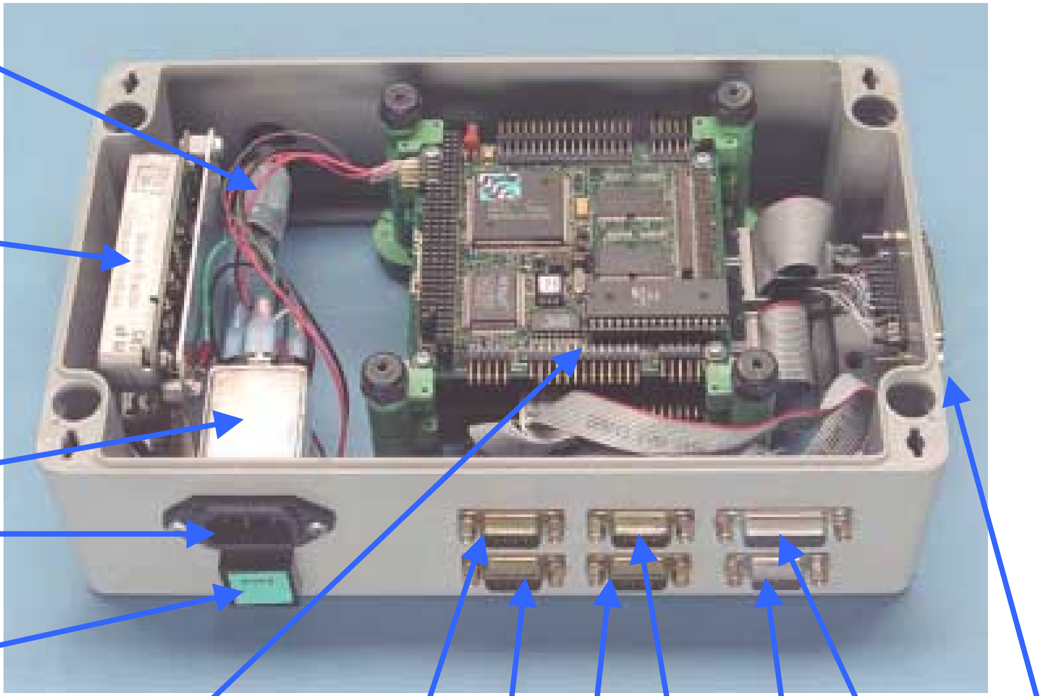
Hardware

- Ampro CoreModule 3SXi – 80386 25-MHz processor card
- Ampro MiniModule SVG-II – Video controller card
- Diamond Systems: Emerald-MM-DIO – I/O card
  - Four COM ports and 48 bits of digital I/O
- Computer case with connectors
- Power Supply (AC to 5 VDC)

Software

- DataLight: ROM-DOS version 6.22 – Operating System
- WCSC: COMM-DRV/LIB version 17.0 – COM Port Driver Software
- LANL: DATA_ATT – Computational Block Software
- Microsoft: MS Visual C version 1.52 – Compiler

Computational Block—Inside-View



Push-Button On/Off Switch

Condor GSC20-5 5V 3.8A switching power supply

Corcom6EC1 Line Filter & AC connector

Fuse

PC/104 Stack

- •Ampro: 3SXi processor card
- •Ampro: SVG-II video card
- •Diamond Systems: Emerald-MM-DIO card

NMC Pu600/300

Pu900 Symmetry

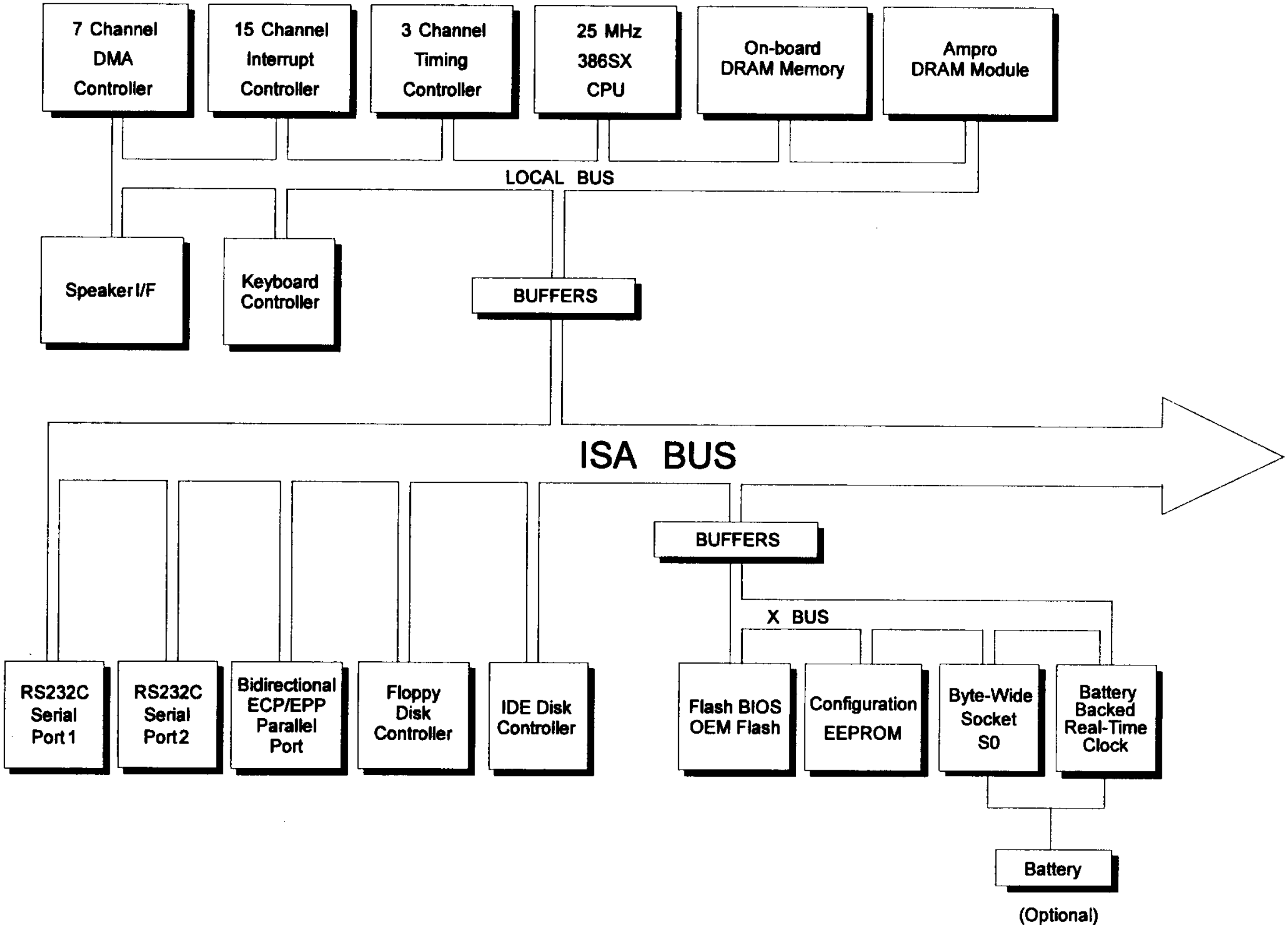
Serial Inputs

Video Output

Control Input

Data Output

AMPRO 3SXi Block Diagram



AMPRO 3SXi Specifications

- 25 MHz 386SX processor
- 2 Mbytes DRAM memory (main memory)
- Shadow RAM support for BIOS
- 14 interrupt channels
- 7 DMA channels
- Three 8254-equivalent programmable timers
- Standard PC/AT keyboard port
- Standard PC speaker port
- Battery-backed real-time clock
- CMOS RAM (support for battery-free operation)
- Award ROM BIOS with Ampro embedded-system extensions
- Two serial ports (COM1 & COM2)(unused)
- One multimode parallel port (LPT)
- Floppy Disk Controller (unused)
- IDE Disk controller (unused)
- 32-pin byte wide memory socket (1.0 Mbyte PROM)
- 2-kbit configuration EEPROM (battery-free boot support)
- Watchdog Timer (trigger hardware reset or NMI)

Random Selection of Equipment

- The concept is that of the host providing the monitor multiple copies of key hardware or software to select for use and for private examination.
- If the measurement system is a relatively inexpensive, portable unit, then random selection by a monitor of complete systems provided by the host is a very powerful method of authentication:
  - allows for detailed private examination of equipment by host at a later time;
  - maximizes confidence of host in system.

Random Selection of Equipment, Continued

- Multiple copies of large, expensive versions of installed systems for random selection is not considered practical.
- For large systems, random selection of key hardware and software elements would also provide the monitor with significant confidence in the fidelity of a host-supplied system.

Random Selection Examples as Applied to the Computational Block

- It should be feasible to have multiple copies of the entire computational block subsystem.
- It should also be feasible to offer key elements of the computational block for random selection:
  - Ampro 3SXi motherboard example
  - Ampro 3SXi source-code-loaded PROM example.

Authentication Using Documentation

- The usefulness of documentation to authenticate complex hardware and software is limited by the complexity of the equipment.
  - This is one reason it is very important to utilize systems that are only as complex as they need to be, systems that have had extraneous functionality removed.
  - The right of the monitor to randomly select any subsystem of a complex system for focused inspection using detailed documentation can be an effective authentication tool.

Authentication Using Documentation, Continued

- The usefulness of detailed documentation for authentication is maximized if the integrated measurement system has been jointly developed.
- The usefulness of hardcopy source code documentation of software for authentication is limited, especially for complex code:
  - machine-readable source code expedites authentication measures;
  - methods and procedures to validate source code and compiled code would be a very good subject for joint development.

Using Documentation to Authenticate the System Configuration

- Hardware
  - – Elements
  - – Interconnections
  - – Switch & jumper settings
  - – Hardware settings made by software
- Software within the CPU
  - – All executable code (in PROM)
  - – BIOS code (in system ROM)
  - – CPU setup parameters (in configuration memory)
  - – Interrupt vectors (in RAM)

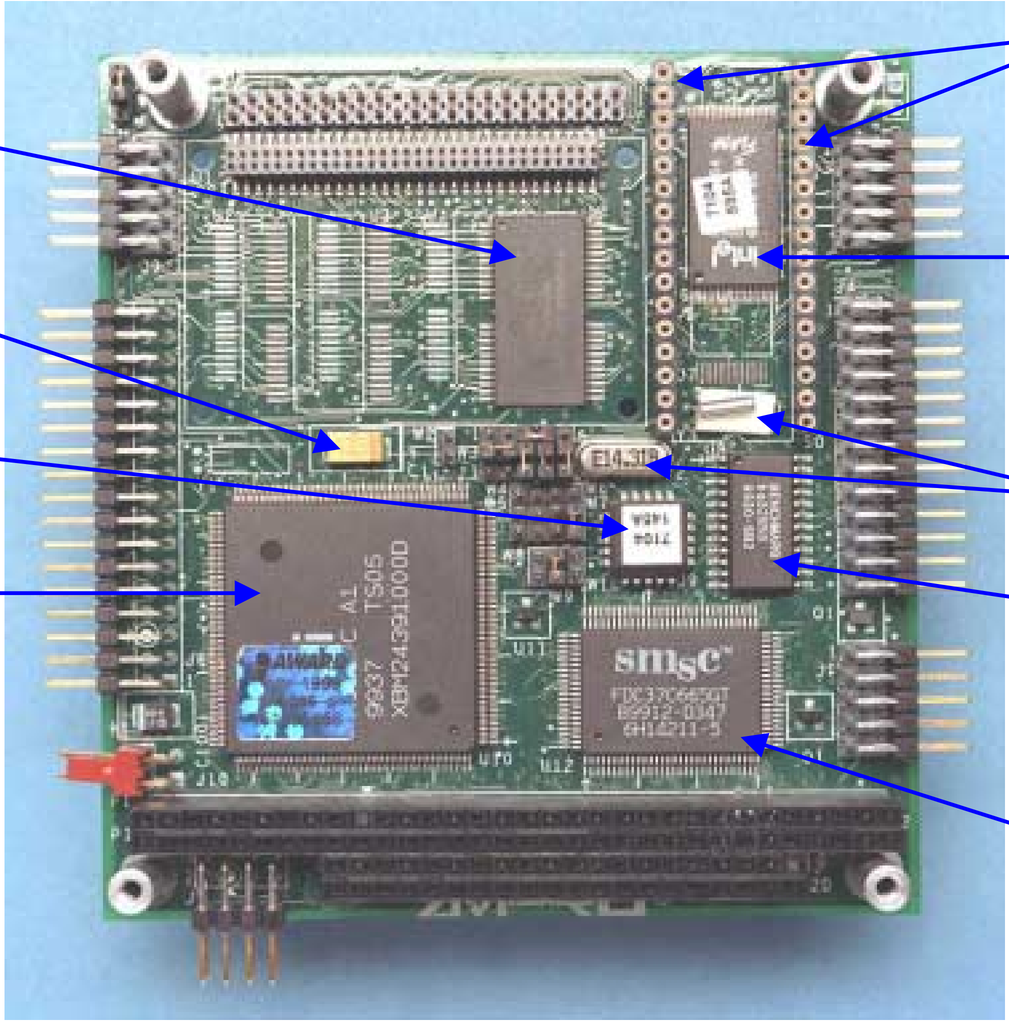
Detailed Computation Block Documentation

Chapter 1	Computational Block Overview
Chapter 2	CPU Card
Chapter 3	Video Card
Chapter 4	Quad COM Port and Digital-I/O Card
Chapter 5	Additional Hardware Support Documentation
Chapter 6	Commercial System Software
Chapter 7	Computational Block Applications Software
Chapter 8	PROM ICs

AMPRO 3SXi Schematics

- Five sheets of Ampro 3SXi schematics are available.
- Possession of schematics requires a nondisclosure agreement with Ampro, Inc.
- Schematics useful for:
    - determining 3SXi parts list,
    - discovering extraneous functionality,
    - jumper functional details,
    - selecting test points.

AMPRO 3SXi
Top View



RAM Memory

Power-on-Reset

Programmable Logic

Embedded Microcontoller 386SX Processor

PROM Memory 32-pin Socket

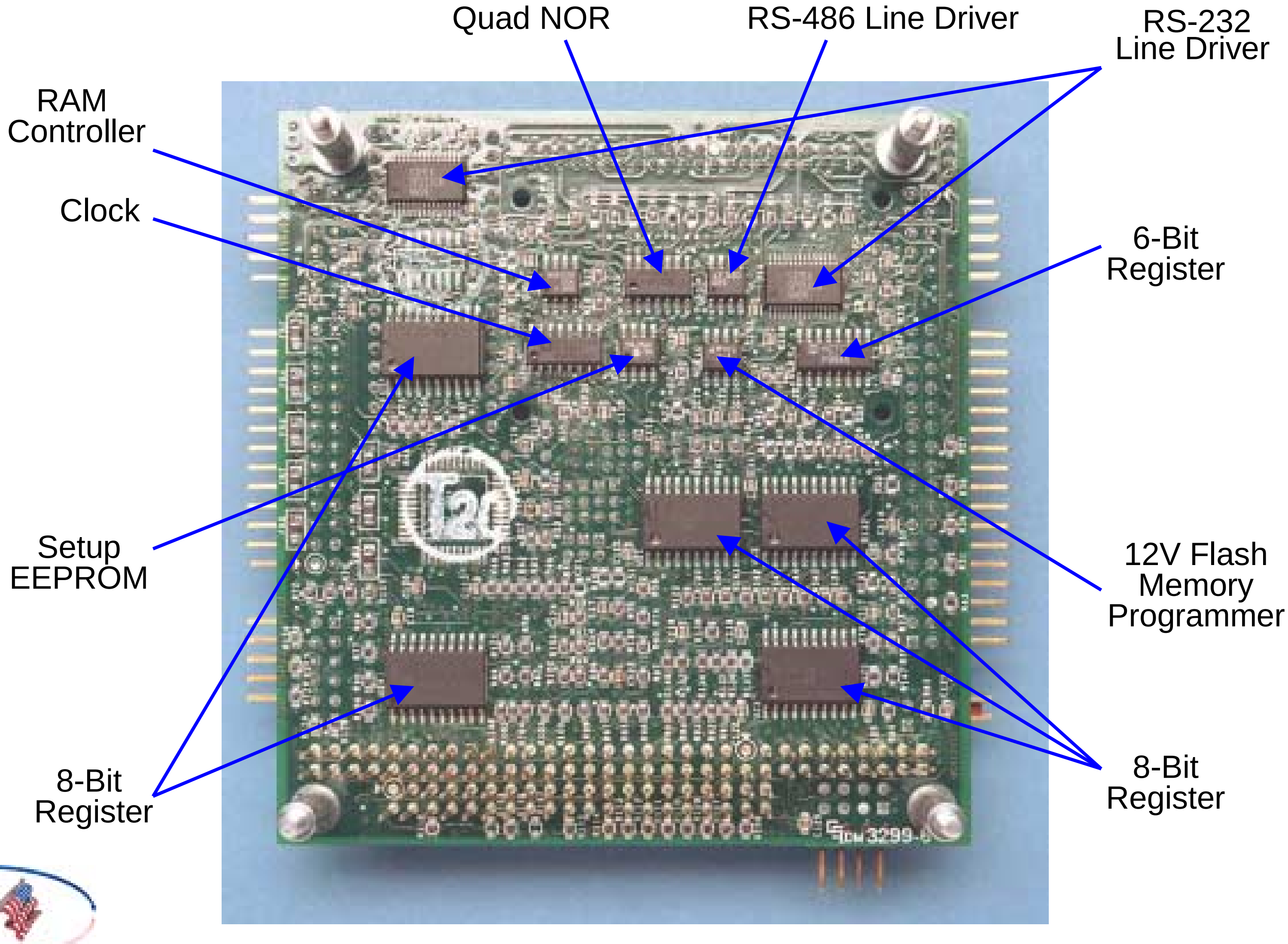
Flash Memory

Clock Crystals

Real-Time Clock

I/O Controller

AMPRO 3SXi Bottom View



Quad NOR

RS-486 Line Driver

RS-232 Line Driver

RAM Controller

Clock

6-Bit Register

Setup EEPROM

12V Flash Memory Programmer

8-Bit Register

8-Bit Register

AMPRO 3SXi Parts List (ICs Only)

Socket	Part: Vendor Part Number
SO	32-pin Socket for 1Mx8 (1-Mbyte) PROM memory — Atmel, AT27C080
U5	1Mx16 (2-Mbyte) RAM Memory — Toshiba, TC5118160CFT-60
U6	1Mx8 (1-Mbyte) Flash Memory — Intel, 28F008SA
U8	Real-Time Clock w/ Setup CMOS Memory — Benchmarq, BQ3285S
U9	Programmable Electrically Erasable Logic (PEEL) Chip — 16V8
U10	Embedded Microcontroller (386SX) — Acer Labs, ALi M6117C
U11	Power-on-Reset Chip — MAXIM, MAX809
U12	I/O Controller — SMSC, FDC37C666GT
U13-14	RS-232 Line Driver — SIPEX, SP211CA
U15	Quad 2-input NOR Gate — Fairchild, 74ACT02
U16	Non-Volatile RAM Controller — MAXIM, MXD1210
U17	Hex D-type Flip-Flop — Harris, 74HCT174
U18	Flash Memory Programming Supply — Linear Technologies, LTC1262
U19	2-kbit Setup EEPROM — Motorola, 93LC56X
U20	Clock Chip — ICS, AV9154-16
U21-23	8-bit Register — Fairchild, 74HCT245
U24	8-bit Register — Motorola, 74HCT244A
U25	RS486 Line Driver — Linear Technologies, LTC485
U35	8-bit Register — Fairchild, 74HCT245

AMPRO 3SXi Mechanical Dimensions

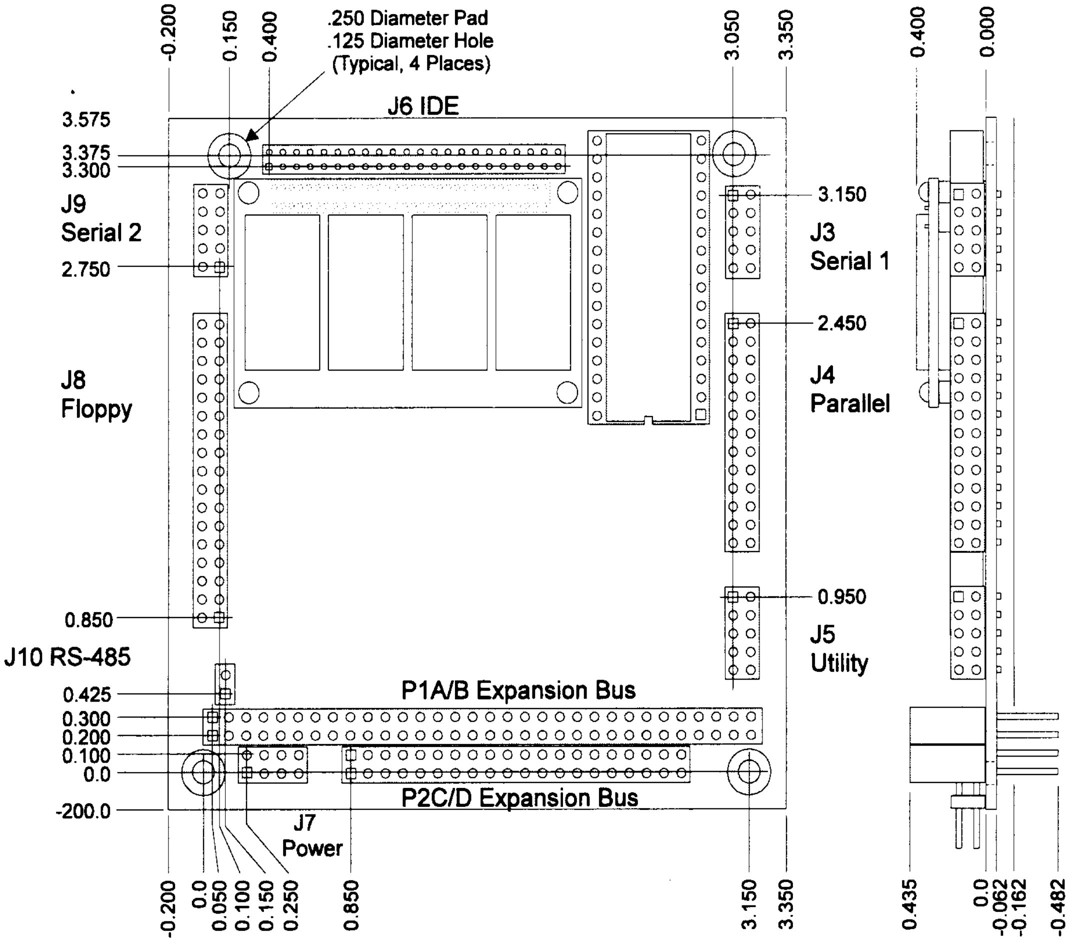
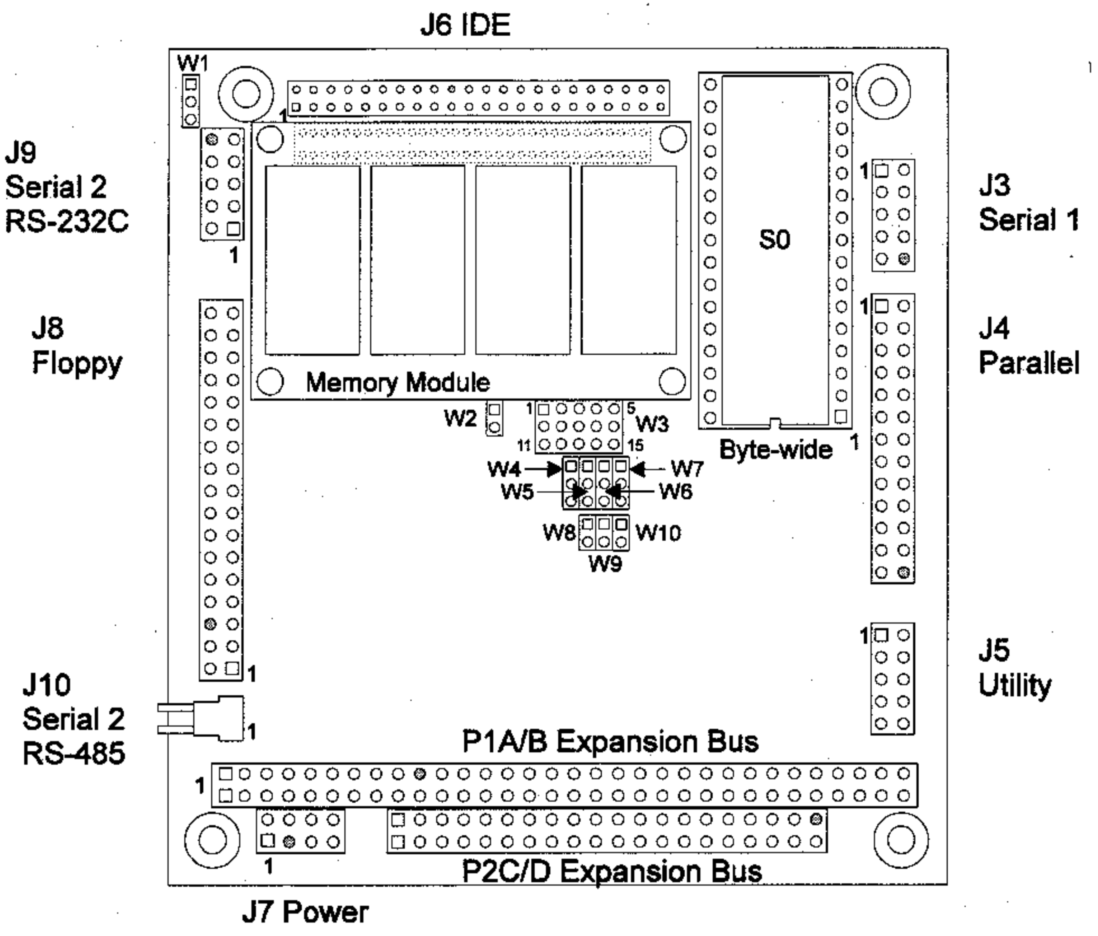


Figure 1–1. Mechanical Dimensions

AMPRO 3SXi Jumper and Connector Locations



(Key pins on connectors are shaded.)

Figure 2–1. Connector and Jumper Locations

AMPRO 3SXi Hardware Jumpers

	FUNCTION	Default	Used	Description
W1	RS-232C/RS-485 Select	1=2	1=2	1=2 COM2 uses RS-232C 2=3 COM2 uses RS-485
W2	BIOS/OEM Flash programming power enable	Off	Off	On = connects V_{pp} for Flash EPROM programming
W3	Byte-Wide Socket Configuration	3=4 6=7 8=13 9=14 10=15	2=7 3=4 9=14 10=15 12=13	15-pins see page 2-23 for EPROM See diagram below 27C080 = 1-Mbyte EPROM used
W4	Watchdog Timer Output Selection [if enabled in SETUP]	Off	Off	1=2 = Hardware Reset 2=3 = I/O Channel Check (NMI) open = IRQ8 turns off interrupt
W5	DMA ACK1/ACK3 For Parallel Port = LPT	Off	Off	1=2 selects DMA channel 1 2=3 selects DMA channel 3
W6	DMA REQ1/REQ3 For Parallel Port = LPT	Off	Off	1=2 selects DMA channel 1 2=3 selects DMA channel 3
W7	Byte-Wide Backup Power Select	1=2	2=3	1=2 enable external battery for SO 2=3 connects device directly to V_{cc}
W8	Byte-Wide Battery Backup Power	Off	Off	On = enables battery backup for memory in SO
W9	BIOS/Byte-Wide Swap	On	On	Off = enables access of a system BIOS from SO
W10	RS-485 Termination	Off	Off	On = 100 ohm terminator

AMPRO 3SXi SETUP.COM Parameters

- 1st Floppy: None
- 2nd Floppy: None
- ATA/IDE Disk 1: None
- ATA/IDE Disk 2: None
- Video: EGA/VGA
- Base Memory: 640
- Extended Memory: 1024
- Error Halt: No Halt
- Video Shadow RAM: Enabled
- System Power on Self Test (POST): Normal
- SCSI BIOS: Disabled
- Extended Serial Config: Disabled
- Extended BIOS: Enabled
- Adv Power Mgmt BIOS: Enabled
- Serial Port 1: Disabled
- Serial Port 2: Disabled
- Parallel Port: Enabled Mode: SPP
- Floppy Interface: Enabled
- IDE Interface: Enabled
- Mono/Color Jumper: Color
- Socket SO: 64K @D0000 hex
- OEM Flash: 64K @DE0000 hex
- Default Socket: SO
- Video State: Enabled
- Blank POST: Enabled
- Serial Boot Loader: Disabled
- Watchdog Timer: Disabled
- Hot Key Setup: Disabled

AMPRO 3SXi I/O Parameters
Interrupts, DMAs & Ports

IRQ	DMA	PORT hex	CARD	FUNCTION
0		040 – 043	3SXi	ROM BIOS clock tick function from programmable timer 3
1		060 – 064	3SXi	Keyboard interrupt
2			3SXi	Cascade for IRQ8-15
3		108 – 10F	DIO	➔ COM2 = PU300/PU600 [3SXi Serial Port 2 IRQ disabled]
4		100 – 107	DIO	➔ COM1 = NMC [3SXi Serial Port 1 IRQ disabled]
5		278 – 27F		2nd LPT
6	2	3F0 – 3F7	3SXi	Floppy controller 8-bit transfers
7		378 – 37F	3SXi	LPT1 = Parallel Port (DMA 1 or 3 possible)
8			3SXi	Reserved for battery-backed clock alarm
9			SVG-2	Video Controller if Jumper W1 On
10		118 – 11F	DIO	➔ COM4 = Symmetry
11		110 – 117	DIO	➔ COM3 = PU900
12				
13				
14		1F0 – 1F7	3SXi	IDE hard disk controller
15				
		300 h	DIO	➔ DIO Port 0 – Input bits from Input switches
		304 h	DIO	➔ DIO Port 4 – Output bits to Display lights
		3052 h	DIO	➔ DIO Port 5 – Output bits to Display lights
		3B4 - 3DA & 46E8	SVG-2	Standard VGA port addresses
	0,1&3			Available for 8-bit transfers
	4			Cascade for DMA channel 0-3
	5,6&7			Available for 16-bit transfers

AMPRO 3SXi Memory Map

ADDRESS RANGE hex	SIZE bytes	FUNCTION
DRAM	1Mx16	2 Mbyte main memory = Toshiba, TC5118160CFT-60
100000 – 1FFFFF	1024k	Extended memory - 1 Mbyte of DRAM
0F0000 – 0FFFFF	64k	Ampro ROM-BIOS – possible shadow copy in RAM
0E0000 – 0EFFFF	64k	Possible memory window into extended memory
0D0000 – 0DFFFF	64k	Flash or Socket memory window into 1 Mbyte of memory
0C0000 – 0CFFFF	64k	Video BIOS – possible shadow copy in RAM for speed
0A0000 – 0BFFFF	128k	Video Screen RAM window into 512k bytes of video DRAM
000000 – 09FFFF	640k	Possible 640-kbytes of DRAM available for programs
		Note: MEM /C memory map required for DRAM details
FLASH	1Mx8	1 Mbyte BIOS & OEM flash memory = Intel, 28F008SA
010000 – 0FFFFF	960k	Unused [010000-01FFFF if 128-kbyte flash Intel 28F010]
000000 – 00FFFF	64k	Ampro BIOS
PROM – A	512kx8	Byte-Wide Socket = 512 kbyte memory = 27F040
000000 – 07FFFF	512k	User files
PROM – B	1Mx8	Byte-Wide Socket =1 Mbyte memory = 27F080
000000 – 0FFFFF	1024k	User files
SETUP EEPROM	256	2-kbit EEPROM = Motorola, 93LC56X
080 – 0FF	128	Documentation is unclear
040 – 07F	64	512 bits for OEM use
000 - 040	64	Setup info
SETUP NVSRAM	128	Real-time clock w/ 114x8 NVSRAM = Benchmarq BQ3285S
00E – 07F	114	Setup storage resisters
000 – 00D	14	Clock & Control Status Resisters

Authenticating PROM Software

- The use of reference radiation sources is the most effective way to check system functionality.
- Random selection of PROMs is probably the most effective way to maximize monitor confidence in the system software.
  - Random selection of PROMs may not be feasible or allowed.
- Other methods to confirm the configuration of installed software exist.
  - All require the generation of a PROM image.
  - Bit-for-bit or hash function comparisons using monitor-supplied laptop computer.
  - “Private” comparisons: host provides the image to the monitor to take home and do with whatever he chooses, (including nothing).